

EXHIBIT B

UNCLASSIFIED



FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Initiate investigation into DDoS attacks against Washburn Computer Group.

Date: 11/17/2015

CC: Robert J. Cameron
TYRA JAMES T

From: MINNEAPOLIS

MP-CY-1

Contact: Brian W. Behm, 763-569-8388

Approved By: SSA Michael J. Krause

Drafted By: Brian W. Behm

Case ID #: 288A-MP-6766321

(U) UNSUB;

Victim: Washburn Computer Group;
Computer Intrusion - Criminal

Synopsis: (U) To open Full Investigation into multiple DDoS attacks against the Washburn Computer Group's website, washburngrp.com.

Full Investigation Initiated: 11/17/2015

Enclosure(s): Enclosed are the following items:

1. (U) Washburn Files

Details:

On 10/13/2015, writer and SA Robert Cameron met with personnel from the Washburn Computer Group (WCG) and LogicNet, LLC at LogicNet's office, located at 8060 MN-55, Rockford, MN. The purpose of the meeting was to discuss the recent multiple distributed denial-of-service (DDoS) attacks targeting WCG's website, washburngrp.com. WCG, which is located at 218 Chelsea Road, Monticello, MN, was represented by Allen Wentland, President, telephone 763.271.3526, email al@washburngrp.com, and Ken Curtis, Vice President, telephone 763.271.3515, email ken@washburngrp.com. LogicNet, which is providing IT support to WCG, was represented by Joel Schmidt and Craig Sixta.

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Initiate investigation into DDoS attacks against Washburn Computer Group.

Re: 288A-MP-6766321, 11/17/2015

WCG sells and repairs point-of-sale equipment to various customers in the retail industry. In approximately 05/2015, LogicNet was engaged by WCG to implement a server for web hosting. Shortly after setting up the server, the washburngrp.com website was targeted by DDoS attacks. After several outages, mitigation services were set up through two different providers. After several weeks of effective mitigation, DDoS attacks resumed and resulted in more outages until filters could be designed to address them, some of which impacted website functionality due to the higher security need. These attacks resulted in several hours of website downtime and potential lost revenue, as well as expenses for consulting on mitigation. At this point, WCG estimated their losses to be between \$3000 and \$5000.

LogicNet provided the following detailed timeline of the events:

- 05/20/2015: VPS setup by LogicNet with LiquidWeb;
- 06/11/2015: washburngrp.com website moved to VPS from prior hosting company;
- 07/30-31/2015: First DDoS attack registered with LiquidWeb;
- 08/10-12/2015: Heavy DDoS attacks;
- 08/12/2015: Changed IP address;
- 08/13/2015: Heavy DDoS attacks;
- 08/14/2015: Incapsula mitigation - two week trial, no outages;
- 08/26/2015: Move to BlockDOS trial - expiration of prior trial, consideration of alternative provider;
- 10/06/2015: Heavy DDoS attacks.

Of note, while two of the DDoS attacks were occurring, WCG Vice President Curtis received emails that appeared to be from a former WCG employee, Loren Stoltenberg. On 08/11/2015, Curtis received an email from loren_stoltenberg@yahoo.com, asking how everything was at WCG. On 10/06/2015, Curtis received an email from lorenstoltenberg15@gmail.com, again asking how everything was at WCG and additionally asking if he needed any IT support. Review of the headers from the two emails did not find any actionable information.

Stoltenberg was employed with WCG for approximately 17 years until he

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Initiate investigation into DDoS attacks against Washburn Computer Group.

Re: 288A-MP-6766321, 11/17/2015

was fired roughly three years ago. Stoltenberg was described as a 'cancer' in the company, and he was fired because he was very difficult to work with. Before the two emails mentioned above, neither Wentland nor Curtis had any contact with Stoltenberg since he was fired three years ago. Stoltenberg was a head technician who primarily performed hardware repairs, however, he was not very experienced with software issues and did not possess the technical background to execute the DDoS attacks described above. In addition, Stoltenberg had a son, Aaron, who was also employed at WCG, but he quit shortly after his father was fired.

When asked if there was anyone else who would want to target WCG, Wentland mentioned his son-in-law, Joe Ayala. Ayala is in the process of getting divorced from Wentland's daughter. Ayala is active duty with the Army and currently stationed in Virginia serving as a Chaplain's assistant. Wentland opined that Ayala's associates through the military would have the capability to carry out a DDoS attack such as what WCG has been experiencing recently. Ayala and Stoltenberg know each other through a common friend, Ron Rearing (ph), who is Wentland's brother-in-law.

LogicNet provided a DVD containing copies of the two emails sent to WCG Vice President Curtis, website uptime logs, Helpdesk Tickets from LiquidWeb providing notification of the attacks, and log files from BlockDOS. Further analysis will be conducted on the log files for any actionable information.

On 11/16/2015, writer briefed the initial case information to Assistant United States Attorney Timothy Rank, who concurred with the opening of captioned investigation.

♦♦

UNCLASSIFIED